

TOTAL ACCESS 600 SERIES T1 TDM IAD User Interface Guide (UIG)

4200681L2	T1 ATM Total Access 608
4200641L2	T1 ATM Total Access 604
4200612L1#ATM	T1 ATM Total Access 612
4200616L1#ATM	T1 ATM Total Access 616
4200624L1#ATM	T1 ATM Total Access 624

April 2002

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.



901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
(256) 963-8000

©2002 ADTRAN, Inc.
All Rights Reserved.
Printed in U.S.A.



Notes provide additional useful information.



Caution signify information that could prevent service interruption.



Warnings provide information that could prevent damage to the equipment or endangerment to human life.

Safety Instructions

When using your telephone equipment, please follow these basic safety precautions to reduce the risk of fire, electrical shock, or personal injury:

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.
2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

Save These Important Safety Instructions

FCC regulations require that the following information be provided in this manual to the customer:

1. This equipment complies with Part 68 of the FCC rules. On the side of the bottom of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN), if applicable, for this equipment. If required, this information must be given to the telephone company.
2. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68-compliant. See installation instructions for details.
3. If your telephone equipment (TA 600) causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice to give you an opportunity to maintain uninterrupted service.
5. If you experience trouble with this equipment (TA 600), please contact ADTRAN for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning.
6. This unit contains no user-serviceable parts.
7. The FCC recommends that the AC outlet to which equipment requiring AC power is to be installed is provided with an AC surge arrester.
8. The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.
9. The following information may be required when applying to your local telephone company for leased line facilities.

Service Type	REN/SOC	FIC	USOC
1.544 Mbps - ESF and B8ZS	6.0N	04DU9-1SN	RJ-48C
Analog Service (Life Line)	0.1B/9.0F	02LS2/02GS2	RJ-11C

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



Shielded cables must be used with this unit to ensure compliance with Class A FCC limits.

WARNING

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Compliance Information

Notice: The Industry Canada label applied to the product (identified by the Industry Canada logo or the “IC:” in front of the certification/registration number) signifies that the Industry Canada technical specifications were met.

Notice: The Ringer Equivalence Number (REN) for this terminal equipment is supplied in the documentation or on the product labeling/markings. The REN assigned to each terminal device indicates the maximum number of terminals that can be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices should not exceed five (5).

Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques,” NMB-003 édictée par le ministre des Communications.

Warranty and Customer Service

ADTRAN will repair and return this product within ten years from the date of shipment if it does not meet its published specifications or fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For service, RMA requests, or further information, contact one of the numbers listed at the end of this section.

LIMITED PRODUCT WARRANTY

ADTRAN warrants that for ten years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to Customer.

Customer Service, Product Support Information, and Training

ADTRAN will repair and return this product if within ten years from the date of shipment the product does not meet its published specification or the product fails while in service.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CAPS) department to have an RMA number issued. CAPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

CAPS Department (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN Customer and Product Service
901 Explorer Blvd. (East Tower)
Huntsville, Alabama 35806

RMA # _____

Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

<http://support.adtran.com>

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

Applications Engineering (800) 615-1176

Post-Sale Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and troubleshooting tools. All of this, and more, is available at:

<http://support.adtran.com>

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

Technical Support (888) 4ADTRAN

Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

<http://www.adtran.com/aces>

For questions, call the ACES Help Desk.

ACES Help Desk (888) 874-ACES (2237)

Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

Training Phone	(800) 615-1176, ext. 7500
Training Fax	(256) 963-6700
Training Email	training@adtran.com

TOTAL ACCESS 600 SERIES T1 TDM IAD USER INTERFACE GUIDE

This document is designed for use by network administrators and others who will configure and provision the Total Access 600 system. It contains overview information, configuration details, menu descriptions, and instructions on navigating the VT 100 user interface.

CONTENTS

Total Access 600 Overview	16
Analog Lifeline	16
Firmware Updates	16
TDM Overview	17
TDM Application	17
Configuring the Total Access 600	18
System Info	18
System Name	18
System Location	18
System Contact	18
Unit Name	18
CLEI Code	18
Part Number	19
Serial Number	19
Firmware Revision	19
Bootcode Revision	19
System Uptime	19
Date/Time	19
System Config	20
Operating Mode	20
T1 Timing Mode	20
Network	20
Telnet Access	20
Telnet User List	20
Name	20
Authen Method	20
Password	20
Idle Time (1-255)	21
Level	21
SNMP Menu	21
Access	21
Communities	21
Name	21
Privilege	21
Manager IP	21
Traps	21
Manager Name	21
Manager IP	21
Maint Port Menu	21

Password Protect	22
Password	22
Baud Rate	22
Data Bits	22
Parity	23
Stop Bits	23
Network Time	23
Server Type	23
SNTP	23
NT Time	23
Active	23
Time Zone	23
Adjust for Daylight Saving	23
Host Address	23
Refresh	23
Status	23
System Utility	24
Upgrade Firmware	24
Transfer Method	24
TFTP Server Address	24
TFTP Server Filename	24
Transfer Status	24
Start Transfer	25
Abort Transfer	25
TFTP Server	25
Config Transfer	25
Transfer Method	25
Transfer Type	25
TFTP Server IP Address	25
TFTP Server Filename	25
Current Transfer Status	26
Previous Transfer Status	26
Load and Use Config	26
Save Config Remotely	26
Ping	26
Start/Stop	26
Host Address	26
Size (40-1500)	26
# of Packets	26
# Transmits	26
# Receives	26
%Loss	26
Configuring the Router – Configuration	27
Global	27
IP	27
Mode	27
Static Routes	28
DHCP Server	28
Domain Names	28

UDP Relay	29
Mode	29
UDP Relay List	29
Bridge	29
Mode	29
Address Table	29
Security	30
Authentication	30
Radius Server	30
Primary Server	30
Secondary Server	30
UDP Port	30
Secret	30
Retry Count (1-10)	30
Filter Defines	30
MAC Filter Defines	31
Pattern Filter Defines	31
IP Filter Defines	31
IPX Filter Defines	33
Ethernet	33
IP	34
IP Address	34
Subnet Mask	34
Default Gateway	34
RIP	35
Proxy ARP	35
IPX	35
Network	35
Frame Type	36
Seed Status	36
RIP Timer (10-180)	36
SAP Timer (10-180)	36
MAC Address	36
WAN	37
L2 Protocol	37
PPP Profile	37
Authentication	37
TX Method	37
TX Username	37
TX Password	37
RX Username	38
RX Password	38
IP	38
Mode	38
Local IP	38
Local Netmask	38
NAT	38
Route	38
RIP	39

IPX	39
Mode	39
Network	39
Triggered	40
Retain	40
Type 20 Packets	40
Bridge	40
Mode	40
Bridge Group	40
PPP	40
VJ Compression	40
Max Config	40
Max Timer	41
Max Failure	41
Filters	41
WAN-TO-LAN (In)	41
In Exceptions	41
LAN-TO-WAN (Out)	42
Out Exceptions	42
Configuring the Router – Status	42
Session	42
ARP cache	42
Bridge Table	42
IP Routes	42
IPX Routes	43
IPX Servers	43
WAN Stats	43
LAN Stats	43
IP Stats	43
Configuring the Router – Logs	43
Sys log Host	44
PPP Log	44
Connection Log	44
Network Log	44
Active	44
Wrap	44
Level	44
View	44
Clear	44
Managing the Modules – Modules	45
NET (T1)	45
Menu	45
Format	45
Line Code	45
Equalization	46
CSU Lpbk	46
Test	46
Loc LB	46
Rem LB	46

Test Status	46
Alarm	46
Loss of Signal (LOS)	46
Red Alarm (RED)	46
Yellow Alarm (YELLOW)	46
Blue Alarm (BLUE)	46
Status	46
Time Frame	46
Clear	46
ES	46
SES	47
SEF	47
FS	47
LCV	47
SLP	47
FXS	47
DS0 Maps	47
Active Map	47
View / Edit Map	47
Use as Template	48
Clear Map	48
Current Map 1	48
Current Map 2	48
D4 Map	48
D1D Map	48
Enter Map	48
DS0	48
Slot	48
Port	49
RBS	49
V.35 Setup	49
Channel Rate	49
CTS	49
DCD	49
DSR	49
Appendix A. Updating Total Access 600 Firmware using XMODEM	50
Updating Firmware via a Forced Download	50
Updating Firmware via the Console Menus	52
Appendix B. Updating Total Access 600 Firmware using TFTP	53
Appendix C. Navigating the Terminal Menus	56
Terminal Menu Window	56
Menu Path	56
Window Panes	56
Window Pane Navigation	57
Right Window Pane Notation	57
Additional Terminal Menu Window Features	57
Navigating Using the Keyboard Keys	57

Moving through the Menus	58
Session Management Keystrokes	58
Configuration Keystrokes	59
Getting Help	59
Appendix D. Configuring the Total Access 600 for Routing	60
Initial Setup	60
DS0 Mapping	60
Setting up Routing Options	61
IP Routing	61
Global IP Setup	61
Ethernet IP Setup	62
WAN IP Setup	63
IPX Routing	65
Global IPX Setup	65
Ethernet IPX Setup	65
WAN IPX Setup	66
IP and IPX Routing	68
Global IP and IPX Setup	68
Ethernet IP and IPX Setup	69
WAN IP and IPX Setup	70
Appendix E. Configuring the Total Access 600 for Bridging	73
Initial Setup	73
Setting up Bridging Options	73
Bridging	73
Global Bridging Setup	73
WAN Bridging Setup	73
No Bridging	74
Appendix F. Configuring the Total Access 600 for Operation with Voice Modules	75
Mapping the DS0s.	75
Setting up the NET (T1) Module	76
Setting up the FXS Voice Ports.	77
Appendix G. Craft Port Connection Pin-Out	78

1. TOTAL ACCESS 600 OVERVIEW

The Total Access™ 600 system (see Figure 1 and Figure 2) is an Integrated Access Device (IAD) designed for cost-effective deployment of voice and data services at the customer premises. The Total Access 600 system benefits integrated communications providers, such as CLEC, ILECs, and ISPs, who required a customer premises device that integrates voice and data functions, and provides a viable migration path from TDM to packet-based technology. The Total Access 600 features remote management and an integrated IP/IPX router. The unit includes a modular network interface, Nx56/64 V.35 interface, 10/100BaseT interface, FXS ports, life-line voice backup, and an optional battery backup for added security. The Total Access 600 can provision, test, and provide status for any of the voice and data interfaces. All connections are made via the rear panel.

Analog Lifeline

The **LIFE LINE** connector on the rear panel (see Figure 1) provides assured voice for port 1. When a network connection is not possible due to loss of power or some other reason, an on-board relay opens and the first port of the voice connector is provided with analog voice from the analog lifeline connection.



For the analog lifeline feature to work, the user must subscribe to an analog voice line and it must be connected via the lifeline connector.

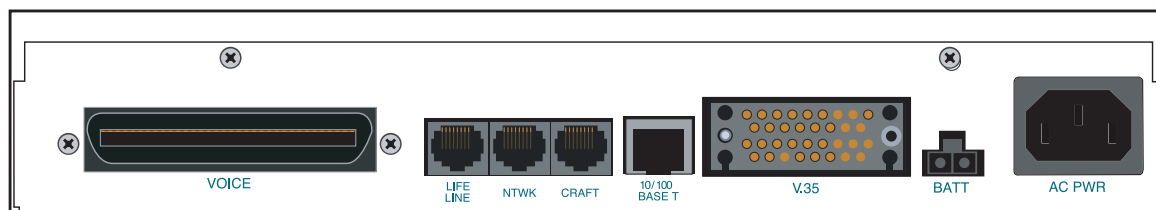


Figure 1. Total Access 600 Rear Panel

Firmware Updates

Firmware can be updated by using XMODEM transfer protocol via the unit's **CRAFT** port (see Figure 1) or by using TFTP from a network server. (See *Appendix A. Updating Total Access 600 Firmware using XMODEM* on page 50 and *Appendix B. Updating Total Access 600 Firmware using TFTP* on page 53.)

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and sub-menus that identify and provide access to specific operations and parameters. These menu selections are described later in this User Interface Guide.



See Appendix C for instructions about navigating the terminal menus.



NOTE

See Appendix G for the **CRAFT** port connection pin-out.

2. TDM OVERVIEW

Time Division Multiplexing (TDM) is the technology used to transmit several separate data, voice, and/or video signals at the same time over one communications path. The path is shared by several channels cyclically by letting each channel use the path exclusively for a short time slot.

3. TDM APPLICATION

Figure 2 shows a typical TDM application. The Total Access 600 connects to the Network to provide both voice and high speed data from a single platform.

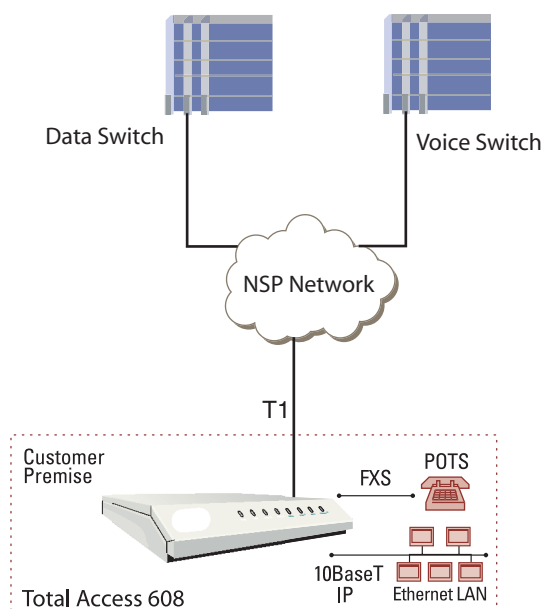


Figure 2. Typical TDM Application



NOTE

Refer to the next section, *Configuring the Total Access 600*, for general configuration instructions. Refer to the appendices at the end of this document for information on using the Total Access 600 in specific applications:

- Appendix D. *Configuring the Total Access 600 for Routing* on page 60.
- Appendix E. *Configuring the Total Access 600 for Bridging* on page 73.
- Appendix F. *Configuring the Total Access 600 for Operation with Voice Modules* on page 75.

4. CONFIGURING THE TOTAL ACCESS 600

System Info

The **SYSTEM INFO** menu provides basic information about the unit and contains data fields for editing information. Figure 3 displays the submenus available when you select this menu item.

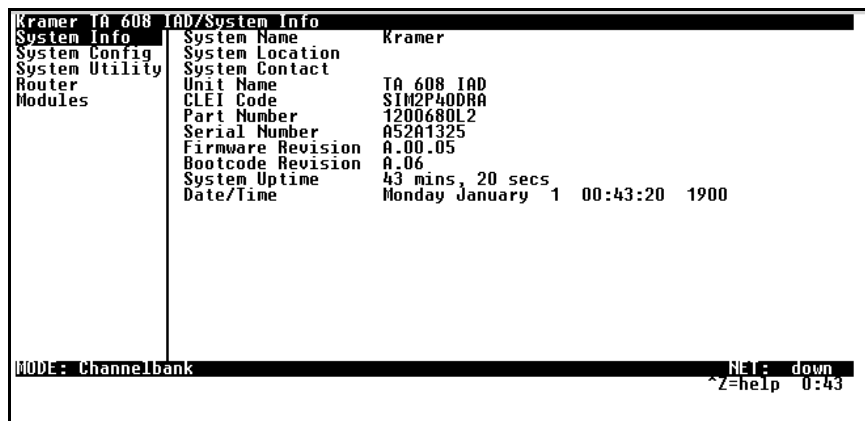


Figure 3. System Information Menu

>System Name

Provides a user-configurable text string for the name of the TA 600. This name can help you distinguish between different installations. You can enter up to 31 characters in this field, including spaces and special characters (such as an underbar). This name will appear on the top line of all screens.

>System Location

Provides a user-configurable text string for the location of the TA 600. This field is to help you keep track of the actual physical location of the unit. You can enter up to 31 characters in this field, including spaces and special characters (such as an underbar).

>System Contact

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the TA 600 system. You can enter up to 31 characters in this field, including spaces and special characters (such as an underbar).

>Unit Name

Product-specific name for the product assembly.

>CLEI Code

CLEI code for the product assembly.

> Part Number

ADTRAN part number for the product assembly.

>Serial Number

Serial number of the product assembly.

>Firmware Revision

Displays the current firmware revision level of the controller.

>Bootcode Revision

Displays the bootcode revision.

>System Uptime

Displays the length of time since the TA 600 system reboot.

>Date/Time

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).



Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

System Config

Set up the Total Access 600 operational configuration from the **SYSTEM CONFIG** menu. Figure 4 shows the items included in this menu.

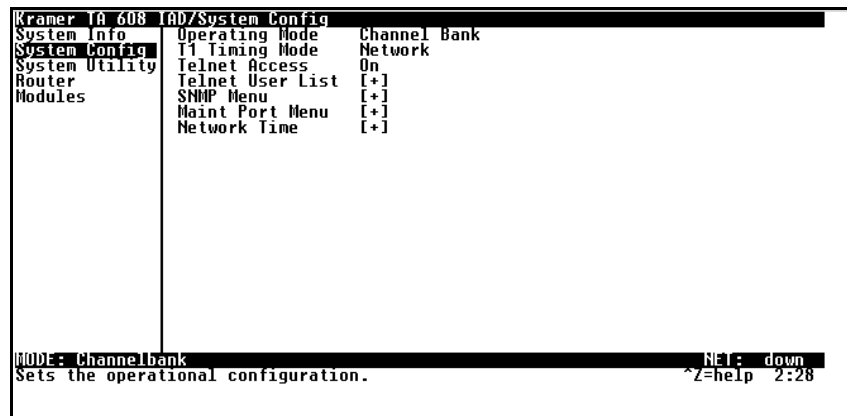


Figure 4. System Configuration Menu

>Operating Mode

>T1 Timing Mode

Selects the timing source for the entire system. Network is the only timing option available.

Network

The system's clock is recovered from the network (WAN interface).

>Telnet Access

Sets Telnet access to **ON** or **OFF**.

>Telnet User List

Up to four users can be configured for access to the Total Access 600. Each user can be assigned a security level and time out.

Name

A text string of the user name for this session.

Authen Method

The user can be authenticated in two ways:

PASSWORD The Password field is used to authenticate the user.

RADIUS The Radius client is used for authenticating the user.

Password

When the authenticating method is **PASSWORD**, this text string is used for the password.

Idle Time (1-255)

This sets the amount of time you can be idle before you are automatically logged off.

Level

This is the security level granted to the user.

>SNMP Menu

The Total Access 600 is an SNMP agent. It can respond to Gets and Sets, and can generate traps. These two lists set up the manager, communities, and levels.

Access

When set to **OFF**, SNMP access is denied. When set to **ON** (def), the Total Access 600 will respond to SNMP managers based on the following lists.

Communities

This list is used to set up to eight SNMP communities names that the Total Access 600 will allow. Factory default sets the community “public” with “Get” privileges.

Name

This is a text string for the community name.

Privilege

The access for this manager can be assigned three levels.

NONE	No access is allowed for this community or manager.
GET	Manager can only read items.
GET/SET	Manager can read and set items.

Manager IP

This is the IP address of SNMP manager. If set to 0.0.0.0, any SNMP manager can access the Total Access 600 for this community.

Traps

The Total Access 600 can generate SNMP traps. This list allows up to four managers to be listed to receive traps.

Manager Name

This is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function.

Manager IP

This is the IP address of the manager that is to receive the traps.

>Maint Port Menu

The Total Access 600's VT 100 **CRAFT** port can be accessed via an RJ-48 located on the rear panel. The setup for these ports is under this menu.

Password Protect

When set to **No**, the maintenance port is not password protected. When **Yes** (def), the Total Access 600 will prompt for a password upon startup.

Password

This is the text string that is used for comparison when password protecting the maintenance port. By default, no password is entered.




If you forget your password, type CHALLENGE in all capital letters. Call technical support and have the displayed CHALLENGE code ready.



The security level for the maintenance port is always set to 0. This gives full access to all menus.



Passwords are case-sensitive.

Instructions for Changing Passwords	
Step	Action
1	Select the PASSWORD field—a new PASSWORD field displays.
2	Type the new password in the ENTER field.
3	Type the new password again in the CONFIRM field.
	<i>The password can contain up to 12 alphanumeric characters. You can also use spaces and special characters in the password.</i>

Baud Rate

This is the asynchronous rate that the maintenance port will run. The possible values are 300, 1200, 2400, 4800, 9600 (def), 19200, 38400, 57600, and 115200.

Data Bits

This is the asynchronous bit rate that the maintenance port will run. The possible values are 7 or 8 (def) bits.

Parity

This is the asynchronous parity that the maintenance port will run. The possible values are **NONE** (def), **ODD**, or **EVEN**.

Stop Bits

This is the stop bit used for the maintenance port. The possible values are 1 (def), 1.5 or 2.

>Network Time

The Total Access 600 unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

Server Type

The server type defines which port the Total Access 600 will listen on to receive timing information from the time server.

SNTP

The Total Access 600 will receive time directly from an SNTP server.

NT Time

The Total Access 600 will receive time from an NT server running SNTP software on its TIME port.

Active

This network timing feature can be turned on and off (by setting to **YES** or **NO**). It determines whether the unit will request and receive time from a time server.

Time Zone

There are several time zones available for the time to be displayed in. All time zones are based off of Greenwich Mean Time (GMT).

Adjust for Daylight Saving

Since some areas of the world use Daylight Savings Time, the Total Access 600 is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on (set to **YES**).

Host Address

This is the IP address of the time server that the Total Access 600 will request and receive time from.

Refresh

This is the interval of time between each request the Total Access 600 sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly, but it is more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit.

Status

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem.

System Utility

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 5.

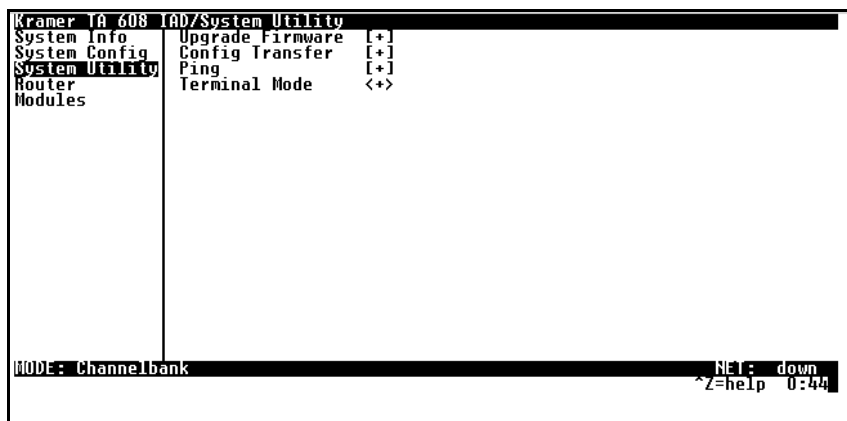


Figure 5. System Utility Menu

>Upgrade Firmware

Updates firmware when TA 600 enhancements are released. Two transfer methods are available for use in updating the Total Access 600 system controller.

Transfer Method

The two methods for upgrading are **XMODEM** and **TFTP**. (See *Appendix A. Updating Total Access 600 Firmware using XMODEM* on page 50 and *Appendix B. Updating Total Access 600 Firmware using TFTP* on page 53 for more information.) **TFTP** requires a TFTP server running somewhere on the network. The Total Access 600 starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the **CRAFT** port using any PC terminal emulator with xmodem capability.

TFTP Server Address

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server.

TFTP Server Filename

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code.

Transfer Status

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

Start Transfer

This activator is used when the configurable items in this menu are complete.



*Before using **START TRANSFER**, the TA 600 should have a valid IP address, subnet mask, and default gateway (if required).*

Abort Transfer

Use this activator to cancel any TFTP transfer in progress.

TFTP Server

Set to **YES** or **NO**.

>Config Transfer

Used only with TFTP transfers. Sends a file containing the TA 600 configuration to a file on a TFTP server using the TFTP protocol. **CONFIG TRANSFER** also lets you save the TA 600 configuration as a backup file, so you can use the same configuration with multiple TA 600 units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the TA 600 called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file. See *Appendix B. Updating Total Access 600 Firmware using TFTP* on page 53 for details on how to use *TFTP Server*.



*Before using **CONFIG TRANSFER**, the TA 600 should have a valid IP address, subnet mask, and default gateway (if required).*

Only one configuration transfer session (upload or download) can be active at a time.

Transfer Method

Displays the method used to transfer the configuration file to or from a server. The choices are **XMODEM** and **TFTP**.

Transfer Type

Only **BINARY** transfers are currently supported.

TFTP Server IP Address

Specifies the IP address of the TFTP server. Get this number from your system administrator.

TFTP Server Filename

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **Total Access 600.cfg**, but you can edit this name.

Current Transfer Status

Indicates the current status of the update.

Previous Transfer Status

Indicates the status of the previous update.

Load and Use Config

Retrieves the configuration file specified in the **TFTP SERVER FILENAME** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.



If you execute this command, the TA 600 retrieves the configuration file, reboots, then restarts using the new configuration.

Save Config Remotely

Saves the configuration file specified in **TFTP SERVER FILENAME** to the server identified in **TFTP SERVER IP ADDRESS**. To start this command, enter **Y** to begin or enter **N** to cancel.



*Before using this command, you must have identified a valid TFTP server in **TFTP SERVER IP ADDRESS**.*

>Ping

Allows you to send pings (ICMP requests) to hosts. The following items are under this menu:



Only one ping session can be active at a time.

Start/Stop

Activator to start and cancel a ping test.

Host Address

IP address or domain name (if DNS is configured) of device to receive the ping.

Size (40-1500)

Total size of the ping to send. Range is 40 (64 is def) to 1500 bytes.

of Packets

Total packets to send every 2 seconds. Setting this to **0** allows the client to ping continuously.

Transmits

Total packets sent (read only).

Receives

Total packets received (read only).

%Loss

Percentage loss based on ping returned from host (read only).

Configuring the Router – Configuration

Use the **ROUTER/CONFIGURATION** menu (Figure 6) to access the **GLOBAL**, **ETHERNET**, and **WAN** menus.

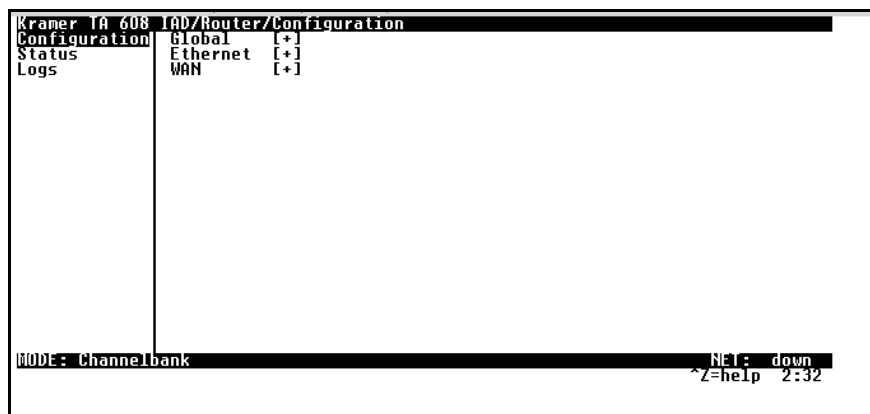


Figure 6. Router/Configuration Menu

>Global

Use the **GLOBAL** menu (Figure 7) to set up general router functions.



Figure 7. Global Menu

IP

This is used for general IP configuration.

Mode

This item controls how the 600 handles IP routes. When this option is set to **ON** (def), the 600 will advertise and listen to routes from other IP routers. If **OFF**, the route table is still used, but only static routes are used for routing IP packets and only the Ethernet port is used. IP packets can be sent over the WAN, but only when bridged.

Static Routes

Use this menu to enter static routes to other networks.

ACTIVE	Adds this static route entry to the IP routing table when set to YES (def) and removes it (if it was previously added) if set to NO .
IP ADDRESS	The IP address of the host or network address of the device being routed to.
SUBNET MASK	Determines the bits in the previous IP address that are used. <i>If this is to be a host route, it must be set to all ones (255.255.255.255).</i>
GATEWAY	The IP address of the router to receive the forwarded IP packet.
HOPS	The number of router hops required to get to the network or host. Maximum distance is 15 hops.
PRIVATE	When set to NO , the Total Access 600 will advertise this static route using RIP. Setting to YES means that the route is kept private.

DHCP Server

DHCP MODE	When set to ON , the Total Access 600 acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the Total Access 600's own IP address and will be within the same network.
DHCP RENEWAL TIME	The number of hours that the DHCP server should allow the device before it is required to send a new DHCP request. The default is 15 hours, and 0 represents an infinite lease.

Domain Names

Enter the 600's domain name and the primary and secondary DNS servers in this menu.

DOMAIN NAME	Text string used to represent the domain name used by the Total Access 600.
PRIMARY DNS	First server to which domain name requests are sent.
SECONDARY DNS	Server used as a backup, in case the primary address does not respond to the request.
PRIMARY NBNS/WINS	Server to which NT domain name requests are sent.
SECONDARY NBNS/WINS	Server used when there is no response from the primary server.

UDP Relay

This menu configures the 600 to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

Mode

When this option is set to **On** (def), the Total Access 600 will act as a relay agent.

UDP Relay List

Up to four relay destination servers can be specified in this list.

RELAY ADDRESS	This is the IP address of the server that will receive the relay packet.
UDP PORT TYPE	
STANDARD (def)	The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123, NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP.
SPECIFIED	When set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).
UDP PORT 1, 2, 3	Used for specifying UDP ports to be relayed. These fields only apply when UDP PORT TYPE is set to SPECIFIED .

Bridge

The **BRIDGE** menu is used to set up the bridge parameters for the 600. The bridging function runs at the Media Access Control (MAC) level which allows any protocol packets that run over Ethernet to be forwarded. Bridging can run concurrently with IP. However, when IP routing is active, IP packets (which include ARP packets) are not bridged.

Mode

This is used to enable the bridge function.

Address Table

The 600 automatically maintains a table of MAC addresses detected and associates those addresses with the LAN or WAN port from which they were received.

AGING	The maximum time an idle MAC address remains in the table before being removed. The value is in minutes.
FORWARD POLICY	When this parameter is set to UNKNOWN (def), any bridge packet with a destination MAC address that is not in the bridge table is forwarded to all other ports. When set to KNOWN , the packet with the unknown destination MAC address is dropped and is not forwarded.

Security

Authentication

The method used for authenticating the PPP peer is selected here. The possible values are:

NONE (def)	No attempt is made to authenticate the PPP peer.
RADIUS	The Total Access 600 will act as a RADIUS client and authenticate the PPP peer using the RADIUS server. The Radius server parameters must be set up properly for this to work.
PPP	The PPP profile is used to authenticate the PPP peer.

Radius Server

The parameters for the RADIUS server are configured in this menu. The RADIUS server can be used for authenticating a PPP peer (if defined under **SECURITY/AUTHENTICATION**) and for Telnet server sessions.

Primary Server

This is the IP address of the first RADIUS server that the Total Access 600 should attempt to communicate with when authenticating a PPP peer.

Secondary Server

This is the IP address of the back-up RADIUS server that the Total Access 600 should attempt to communicate with when the primary server does not respond.

UDP Port

This is the UDP port that the Total Access 600 should use when communicating with the RADIUS server. The default is 1645, which is the commonly used port.

Secret

The RADIUS server and Total Access 600 share this text string. It is used by the RADIUS server to authenticate the Total Access 600, the RADIUS client. The factory default is not to use a secret.

Retry Count (1-10)

This is the number of times the Total Access 600 should send a request packet to the RADIUS server without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the secondary server (if defined) is tried. If the secondary server does not respond within the retry count, the PPP peer (or Telnet session) is not authenticated and is dropped. The default is 5.

Filter Defines

The Total Access 600 can filter packets based on certain parameters within the packet. The method used by the Total Access 600 allows the highest flexibility for defining filters and assigning them to a PVC. The filters are set up in two steps: (1) defining the packet types, and (2) adding them to a list under the PVC. This menu is used to define the individual filter defines based on packet type.

MAC Filter Defines

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the Total Access 600 are defined here. Up to 32 MAC defines can be specified.

NAME	Identifies the filter entry.
SRC ADDR	48-bit MAC source address used for comparison. (hexadecimal format)
SRC MASK	Bits in the MAC source address which are compared. (hexadecimal format)
DEST ADDR	48-bit MAC destination address used for comparison. (hexadecimal format)
DEST MASK	Bits in the MAC destination address used for comparison. (hexadecimal format)
TYPE	16-bit MAC type field used for comparison. (hexadecimal format)
TYPE MSK	Bits in the MAC type field used for comparison. (hexadecimal format)

Pattern Filter Defines

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the Total Access 600. Up to 32 pattern defines can be specified.

NAME	Identifies the filter entry.
OFFSET	Offset from beginning of packet of where to start the pattern comparison.
PATTERN	64 bits used for comparison. (hexadecimal format)
MASK	Bits in the pattern to be compared. (hexadecimal format)

IP Filter Defines

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

NAME	Identifies the filter entry.
SRC ADDR	IP address compared to the source address. (dotted decimal format)
SRC MASK	Bits which are used in the source comparison. (dotted decimal format)
DEST ADDR	IP address compared to the destination address. (dotted decimal format)
DEST MASK	Bits which are used in the destination comparison. (dotted decimal format)

SRC PORT	IP source port number used for comparison Range: 0 to 65535. (decimal format)
SRC PORT COMP	Type of comparison that is performed. = means ports equal to not = means port not equal to > means port greater than < means port less than None - means the source port is not compared
DEST PORT	IP destination port number used for comparison Range: 0 to 65535. (decimal format)
DEST PORT COMP	Type of comparison that is performed = means ports equal to not = means port not equal to > means port greater than < means port less than None - means the destination port is not compared
PROTO PORT	Protocol used for comparison. Range: 0 to 255. (decimal format)
PROTO PORT COMP	Type of comparison that is performed = means protocols equal to not = means protocols not equal to > means protocols greater than < means protocols less than None means the protocol is not compared
TCP EST	Yes - only when TCP established No - only when TCP not established Ignore - ignore TCP flags

IPX Filter Defines

The IPX filter defines apply to any IPX packet whether it is routed or bridged. Also, any IPX encapsulation type will be accounted for. Up to 32 IPX defines can be specified.

NAME	Identifies the filter entry (15 characters max)
SRC NET	32-bit source network address
SRC MASK	Bits in the source network address which are compared. (hexadecimal format)
DEST NET	32-bit destination network address
DEST MASK	Bits in the destination network address which are compared. (hexadecimal format)
SRC SOCKET	16-bit value which is the source socket. Range: 0-65535.
SRC SOCKET COMP	Type of comparison that is performed: = means socket equal to not = means socket not equal to > means socket greater than < means socket less than none = no comparison is done on source socket
DEST SOCKET	16-bit value which is the destination socket. Range: 0-65535.
DEST SOCKET COMP	Type of comparison that is performed: = means socket equal to not = means socket not equal to > means socket greater than < means socket less than none = no comparison is done on destination socket
TYPE	8-bit value which is the IPX type
TYPE COMP	Type of comparison that is performed: = means type equal to not = means type not equal to > means type greater than < means type less than none = no comparison is done on IPX type

>Ethernet

Use the **ETHERNET** menu (Figure 8) to configure the Ethernet port on the 600.



Figure 8. Ethernet Menu

IP

This is used to set up the IP addresses for the LAN on the 600

IP Address

The IP address assigned to the 600's Ethernet port is set here. This address must be unique within the network.

Subnet Mask

This is the IP network mask that is to be applied to the 600's Ethernet port.

Default Gateway

The default gateway is used by the 600 to send IP packets whose destination address is not found in the route table.

RIP

Use this menu to enable RIP on the LAN interface.

MODE	Enables or disables RIP.
PROTOCOL	Specifies the RIP protocol. Choices are V1 (def) (which is RIP version 1) or V2 (RIP version 2).
METHOD	Specifies the way the RIP protocol sends out its advertisements. Choices are given below.
NONE	All routes in the router table are advertised with no modification of the metrics.
SPLIT HORIZON (def)	Only routes not learned from this circuit are advertised.
POISON REVERSE	All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric.
DIRECTION	Allows the direction at which RIP advertisements are sent and listened to be specified.
TX AND RX (def)	RIP advertisements are periodically transmitted and are listened to on this port.
TX ONLY	RIP advertisements are periodically transmitted but are not listened to on this port.
RX ONLY	RIP advertisements are not transmitted on this port, but are listened.
V2 SECRET	Enter the secret used by RIP version 2 here.

Proxy ARP

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES**, when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the 600 will answer the request with its own hardware address.

IPX

This menu is used to set up the IPX parameters for the Total Access 600. Any general IPX-related configuration item can be found under this menu.

Network

The IPX network address for the Ethernet port is set here. This is an eight-digit hexadecimal value that uniquely identifies the network segment of the Ethernet port. Accidental selection of an IPX network which is already in use on another network segment may cause hard-to-diagnose problems. IPX network numbers should be carefully tracked.

Frame Type

The Total Access 600 supports all four defined IPX frame types. The possible frame types are: **Ether Type II** (def), **Ether 802.3 (Raw)**, **Ether 802.2**, or **Ether SNAP** (802.2 SNAP). Only one frame type can be used at one time.

Seed Status

The seed status defines what the Total Access 600 is to do with the network information on the selected frame type during startup. There are three possible seeding selections specified:

SEED	The Total Access 600 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Total Access 600 will use the configured IPX network number for the Ethernet segment.
NON-SEED (DEF)	The Total Access 600 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Total Access 600 will wait indefinitely until a number is sent by another router on the Ethernet segment.
AUTO-SEED	The Total Access 600 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Total Access 600 will auto-generate a valid number using its routing tables.

RIP Timer (10-180)

This value specifies how often the Total Access 600 sends out IPX RIP packets on the network segment attached to the Ethernet port. The RIP packets sent contain routing information about the networks for which this Total Access 600 is responsible. The default value is 60 seconds.

SAP Timer (10-180)

This value specifies how often the Total Access 600 sends out IPX SAP (Service Access Protocol) packets on the network segment attached to the Ethernet port. The SAP packets sent contain information about the services (such as servers, printers, etc.) for which this Total Access 600 is responsible. The default value is 60 seconds.

MAC Address

This is a read-only MAC address programmed at ADTRAN.

>WAN

Use the **WAN** menu (Figure 9) to configure WAN settings on the 600.

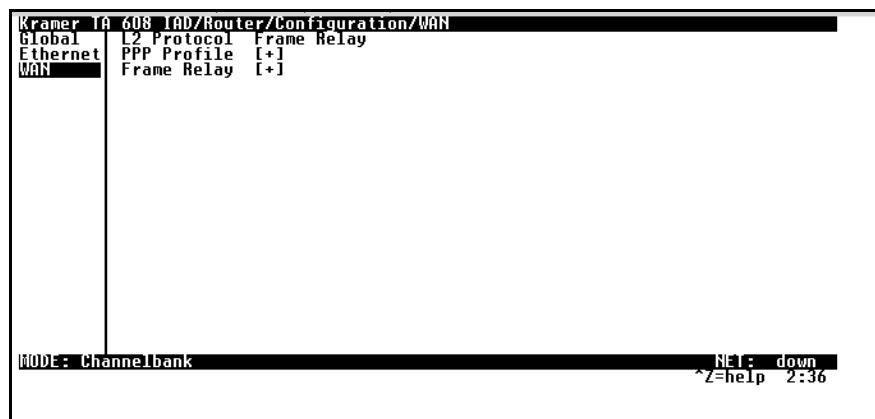


Figure 9. WAN Menu

L2 Protocol

Select the L2 protocol (PPP or Frame Relay).

PPP Profile

The Total Access 600 uses the PPP profile to specify the profile used when connected using PPP.

Authentication

The authentication menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the Total Access 600 and the PPP peer as follows:

TX Method

This parameter specifies how the Total Access 600 is to be authenticated by the PPP peer. There are four possible selections.

NONE (def)	The connection will not allow the PPP peer to authenticate it.
PAP, CHAP, OR EAP	The connection can be authenticated using PAP, CHAP or EAP.
CHAP OR EAP	The connection can be authenticated using CHAP or EAP only.
EAP	The connection will only allow authentication by the peer using EAP.

TX Username

This is the username that is used when being authenticated by the PPP peer.

TX Password

This is the password or secret that is used when being authenticated by the PPP peer.

RX Username

This is the username used to authenticate the PPP peer.

RX Password

This is the password or secret that is used to authenticate the PPP peer.

IP

The IP menu contains the parameters for exchanging IP data with the PPP peer.

Mode

Setting to **ON** (def) will permit this connection profile to negotiate PPP IPCP with the PPP peer for exchanging of IP packets.

Local IP

This is the IP address that is assigned to the PPP link when using numbered links. Leaving this as 0.0.0.0 means the Total Access 600 will determine its IP address using PPP IPCP. If the far end router does not assign an IP address, the PPP link is left unnumbered.

Local Netmask

This network mask is applied to the IP/Local IP address for determining the PPP peer's network. If left as 0.0.0.0, a standard network mask is used.

NAT

The Total Access 600 can perform Network Address Translation. This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is connected, all IP addresses on the Ethernet side are translated into the one real IP address negotiated with the PPP peer (ISP). Multiple stations on the Ethernet side can access the Internet simultaneously. Setting this option to **ON** will cause the Total Access 600 to perform NAT. In the **OFF** (def) position, the unit will route across the connection normally.

Route

The IP parameters are configured in this menu. Usually the Total Access 600 will automatically discover the PPP peer's networks using PPP IPCP and/or RIP.

• **Remote IP/Net**

The PPP peer's IP address or network can be set here, if known. Leaving this at 0.0.0.0 means that the Total Access 600 will determine the PPP peer's IP and network using the PPP IPCP.

• **Remote Netmask**

This network mask is applied to the **IP/NET** address for determining the PPP peer's network. If left as 0.0.0.0, a standard network mask is used.

• **Static Route**

Selecting **YES** will add a static route to the remote peer to the route table.

• **Private**

Selecting **YES** will prevent this route from being advertised.

• **Hops (1-16)**

This value is the metric or number of hops that RIP will use in advertising the static route. The range is 1 to 16, where 1 is the default. The value 16 is considered an infinite distance (poisoned route).

- **Force IP**

When set to **YES**, the Total Access 600 will force the PPP peer to use the IP address in the **LOCAL IP** for this profile as its WAN IP address. Normally, this is set to **NO** (def).

RIP

The RIP parameters can be adjusted from their defaults under this menu.

- **Mode**

The Total Access 600 performs RIP over the WAN connection when this is set to **ON** (def).

- **Protocol**

The Total Access 600 performs version 1, **V1** (def), or version 2, **V2**, of RIP on this WAN connection.

- **Method**

SPLIT HORIZON	Only routes not learned on the WAN connection are advertised.
POISON REVERSE (def)	All routes are advertised, including routes learned from the WAN connection. These routes are poisoned.
NONE	All routes are advertised, including routes learned from the WAN connection. No attempt is made to poison these routes.

- **Direction**

TX AND Rx (def)	RIP advertisements are transmitted and listened to on the WAN connection.
TX ONLY	RIP advertisements are transmitted and not listened to.
RX ONLY	RIP advertisements are listened to but not transmitted.

- **Triggered**

When set to **YES**, only IP RIP updates are sent when the routing table has changed and learned routes are not "aged." When set to **NO** (def), updates are sent periodically.

- **Retain**

When this Connection List entry is disconnected and this parameter is set to **YES**, all routes learned from this WAN connection are retained and their routing interface is set to idle.

IPX

The IPX menu contains the parameters for exchanging IPX data with the PPP peer.

Mode

Setting to **ON** (def) will permit this connection profile to negotiate PPP IPXCP with the PPP peer for exchanging of IPX packets.

Network

A non-zero value in this network number will allow the TA600 to add a route to the PPP peer's network to the routing table.

The Total Access 600 normally will treat the WAN network as an unnumbered link. This is usually referred to as being a “half-router.” However, a PPP peer which wants to assign a network address to the WAN link can do so, in which case the Total Access 600 will go into “full-router” mode.

Triggered

When set to **YES**, only IPX RIP and SAP updates are sent when the routing or service table has changed and learned routes are not “aged.” When set to **NO** (def), updates are sent periodically based on the RIP and SAP timers set in **CONFIGURATION/IPX/RIP TIMER** and **CONFIGURATION/IPX/SAP TIMER**.

Retain

When this Connection List entry is disconnected and this parameter is set to **YES**, all routes learned from this WAN connection are retained and their routing interface is set to idle.

Type 20 Packets

For certain protocol implementations, like NetBIOS, to function in the NetWare environment, routes must allow a broadcast packet to be propagated throughout the IPX networks. The Type 20 IPX packet is used specifically for this purpose. This causes special handling of this packet by the Total Access 600. When a router receives this type of packet, it rebroadcasts it across all interfaces except the one it is received on and includes the network number of that interface in the data portion of the packet. The IPX Router Specification from Novell notes that Type 20 packets should not be propagated across slower links with bandwidths of less than 1Mbps (like ISDN). However, when set to **PASS** (def), the Total Access 600 will allow these packets to propagate over the WAN connection. This facilitates dial-on-demand applications. When set to **BLOCK**, all Type 20 packets are not propagated across the WAN connection.

Bridge

The Bridge menu contains the parameters needed for exchanging bridged packets with the PPP peer.

Mode

When set to **ON**, the Total Access 600 will attempt to negotiate PPP BCP with the PPP peer. Bridging can be used even in route mode only if the PPP peer cannot support certain PPP protocols for that particular routing protocol.

Bridge Group

The specified bridge group (**GROUP 1** or **GROUP 2**). These groups correspond to the spanning tree protocols Bridge Group 1 and Bridge Group 2.

PPP

The Total Access 600 supports the IETF standards for the Point-to-Point Protocol. The PPP state machine running in the Total Access 600 can be fine-tuned to support many applications that can be employed. The configurable items under this menu can be changed from their default values for special cases.

VJ Compression

When this item is set to **ON**, the Total Access 600 will perform TCP/IP header compression known as Van Jacobson compression to the PPP peer.

Max Config

This value is the number of unanswered configuration-requests that should be transmitted before giving up on a call. The possible values are 5, 10 (def), 15 and 20.

Max Timer

This value is the number of seconds to wait between unanswered configuration requests. The possible values are 1 sec, 2 secs (def), 3 secs, 5 secs and 10 secs.

Max Failure

Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. This allows a connection to succeed that might otherwise fail. The possible values are 5 (def), 10, 15 and 20.

Filters

The Total Access 600 can block packets in and out of a WAN port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **CONFIGURATION/GLOBAL/SECURITY/FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

WAN-TO-LAN (In)

The packets which come into the Total Access 600 can be filtered in three ways:

DISABLED (def)	Turns off packet input filtering. No incoming packets are blocked.
BLOCK ALL	All incoming packets from the WAN are blocked except as defined in the FILTERS/IN EXCEPTIONS list.
FORWARD ALL	All incoming packets from the WAN are not blocked except as defined in the FILTERS/IN EXCEPTIONS list.

In Exceptions

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

ACTIVE	Turns this entry active when set to ON .
TYPE	Selects the filter define list to reference:
MAC	from the CONFIGURATION/GLOBAL/SECURITY/FILTER DEFINES/MAC FILTER DEFINES list.
PATTERN	from the CONFIGURATION/GLOBAL/SECURITY/FILTER DEFINES/PATTERN FILTER DEFINES list.
IP	from the CONFIGURATION/GLOBAL/SECURITY/FILTER DEFINES/IP FILTER DEFINES list.
IPX	from the CONFIGURATION/GLOBAL/SECURITY/FILTER DEFINES/IPX FILTER DEFINES list.
FILTER LIST NAME	Selects between filters defined in the list.
NEXT OPER	The next operation to use to combine with the next filter in the list:
END	the last filter to combination.
AND	logically AND this filter with the next filter in the list.
OR	logically OR this filter with the next filter in the list.

LAN-TO-WAN (Out)

The packets which come out toward the WAN from the TA600 can be filtered in three ways:

DISABLED (def)	Turns off packet input filtering. No outgoing packets are blocked.
BLOCK ALL	All outgoing packets to the WAN are blocked except as defined in the FILTERS/OUT EXCEPTIONS list.
FORWARD ALL	All outgoing packets to the WAN are not blocked except as defined in the FILTERS/OUT EXCEPTIONS list.

Out Exceptions

This is a list of up to 32 filter entries. The setup is exactly the same as the **FILTERS/IN EXCEPTIONS** list.

Configuring the Router – Status

Use the **ROUTER/STATUS** menu to view and set the parameters shown in Figure 10. The **ROUTER/STATUS** screens give the user useful information for debugging the current routes in the 600.

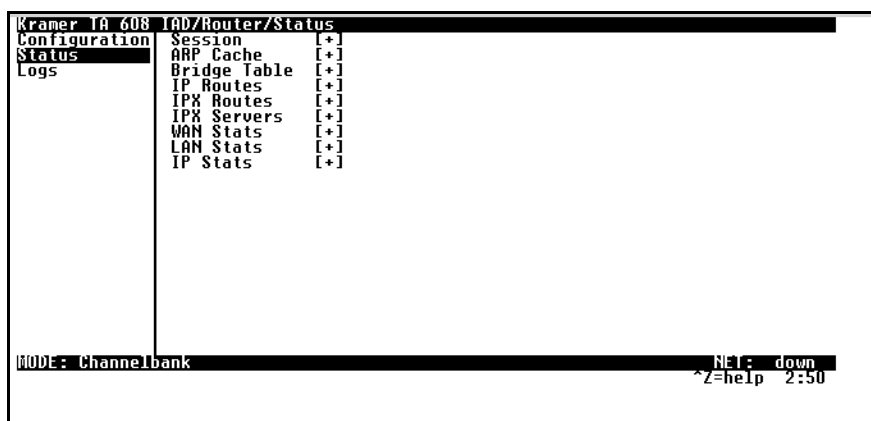


Figure 10. Router/Status Menu

>Session

This menu maintains statistics about the active ATM PVCs.

>ARP cache

This is a listing of the currently connected Ethernet port on the LAN.

>Bridge Table

This shows the detected MAC addresses and the interface to which they are associated.

>IP Routes

This shows the current routes in the 600 and their use.

>IPX Routes

This shows the current routes in the 600 and their use.

>IPX Servers

This shows the current servers in the 600 and their use.

>WAN Stats

This shows the traffic over the WAN interface.

>LAN Stats

This shows traffic over the LAN interface.

>IP Stats

This shows IP traffic through the 600.

Configuring the Router – Logs

The Logs menu (Figure 11) contains logs displaying important information about the running condition of the Total Access 600. The logs can be set to capture diagnostics of error conditions only by way of a log level. The levels are divided up as follows:

- level 0 - Fatal event (causes reset)
- level 1 - Critical event
- level 2 - Error event
- level 3 - Warning event
- level 4 - Notify event
- level 5 - Informational event
- level 6 - Debugging event



Figure 11. Router/Logs Menu

Sys log Host

Set this to the IP address or domain name (if DNS configured) of the sys log host device. All log events are sent to this device.

PPP Log

Information pertaining to the PPP negotiation and authentication is logged in the PPP log.

Connection Log

Information pertaining to the call placement and answering is logged in the Connection log.

Network Log

Information pertaining to routing protocols is placed in this log.

Each log (PPP log, Connection log, and Network log) contains the following elements.

Active

When set to **YES** (def), PPP events below or equal the log level are logged into the log.

Wrap

When set to **YES** (def), new PPP events will overwrite old PPP events when the log is full. All logging will stop when the log is full and set to **NO**.

Level

In order to log events, they must be at or below this level. Range is 0 to 6. The default is 3.

View

This menu displays the log list. The fields are as follows:

DATE/TIME	Date and time event occurred.
LEVEL	Level associated with this event (0-6).
MESSAGE	Text message for this event. If message is too long to fit on the line, another event appears below it continuing the message.

Clear

This clears the log when activated.

Managing the Modules – Modules

Use the **MODULES** menu to view and set the parameters shown in Figure 12. The Total Access 600 contains four integrated modules: The WAN/Network interface, FXS, Echo Cancellor/ADPCM module, and the V.35 interface. The **MODULES** table allows management of the on-board modules in the Total Access 600.

The table contains **MENU**, **ALARM**, **TEST**, and **STATUS** indicators/menus customized for each module.

Kramer TA 608 IAD/Modules/Modules						
Modules	Slot	Type	Menu	Alarm	Test	Status
DSO Maps	0	NET (T1)	[+]	[+]	[+]	[+]
V.35 Setup	1	FXS	[+]	[n/a]	[+]	[+]

MODE: Channelbank	NET: down
Access module menus	^Z=help 0:45

Figure 12. Modules Menu

>NET (T1)

Menu

Format

Sets the frame format for the T1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** (extended superframe), **SF** (superframe), or **SLC96 ALARM 1-16**, or **SLC96 ALARM 1-13**.



SF is equivalent to the D4 frame format.

Line Code

Sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) or **AMI** (alternate mark inversion).

Equalization

Sets the line build-out for the T1 interface. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. Choices are 0dB,-7.5dB,-15dB,-22dB,266FT,399FT,533FT,and 655 FT.

CSU Lpbk

Enables or disables far-end commanded loopbacks via the FDL channel.

Test

These options are used to initiate local and remote loopback tests and display the test status.

Loc LB

(Local Loopback) Causes loopback on near-end port.

Rem LB

(Remote Loopback) Sends a loopback code to a remote CSU.

Test Status

Indicates whether a test is underway.

Alarm**Loss of Signal (LOS)**

No signal detected on port interface.

Red Alarm (RED)

Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF).

Yellow Alarm (YELLOW)

Remote alarm indicator (RAI) being received on port.

Blue Alarm (BLUE)

Receiving unframed all ones from the port alarm indicator signal (AIS).

Status

Displays T1 performance data.

Time Frame

In the Time Frame menu, three options are available: **CURRENT** , **15 MIN** and **24 HR**. The performance data for the given window is stored.

Clear

Clears information for the selected port. Press **ENTER** when the cursor is over this field to clear the data.

ES

Errored Seconds. An ES is a second with one or more error events or one or more Out Of Frame events or one or more Controlled Slips.

SES

Severely Errored Seconds. An SES is a second with 320 or more error events or one or more OutOf-Frame events.

SEF

Severely Errored Frames.

FS

Frame Sync Errors.

LCV

Line Code Violations.

SLP

Slip Error Events.

>FXS

Refer to the Total Access 600 Series FXS Voice Ports User Interface Guide.

DS0 Maps

The **DS0 MAPS** menu allows you to map data and voice ports to the network T1 time slots. You can edit one of two maps stored in nonvolatile memory and make one of the maps the currently active map. Figure 13 on page 47 shows the **CHANNEL BANK/DS0 MAPS** menu.

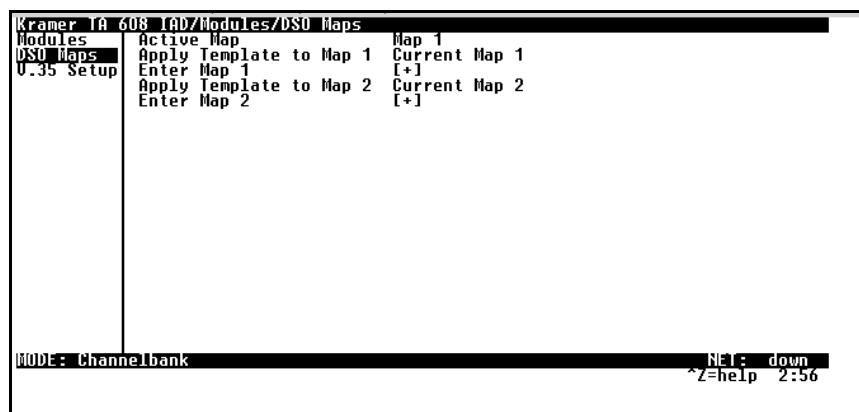


Figure 13. DS0 Maps Menu

Active Map

Activates one of the two dedicated maps (**MAP 1** or **MAP 2**).

View / Edit Map

This field indicates the map that is to be viewed or edited when **ENTER MAP** is pressed: **MAP 1** or **MAP 2**.

Use as Template

This field defines the template to be used when viewing or editing a map. The template is used to create a temporary copy of the map which can be viewed or edited. When the menu is exited, the user has the option of saving the temporary copy back to the actual map.

Clear Map

Unassigns all time slots.

Current Map 1

Uses the currently defined Map 1.

Current Map 2

Uses the currently defined Map 2.

D4 Map

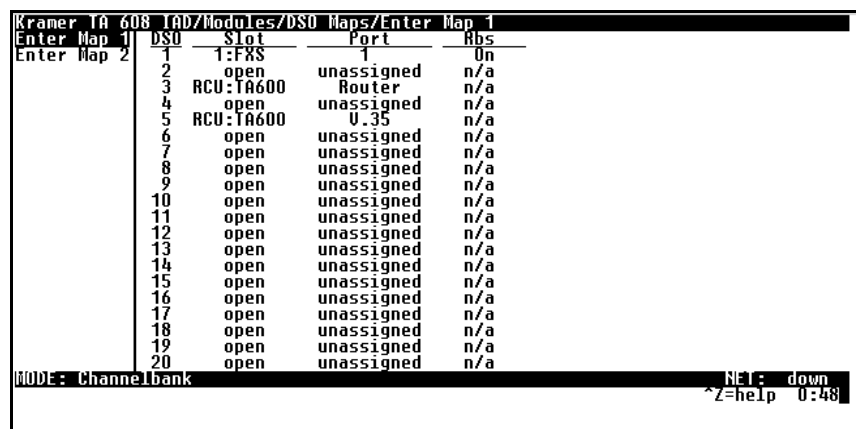
Uses the D4 channel bank definition to assign time slots.

D1D Map

Uses the D1D channel bank definition to assign time slots.

Enter Map

Enters the selected map. (See Figure 14 on page 48.)



The screenshot shows a terminal window with the title 'Kramer TA 608 IAD/Modules/DSO Maps/Enter Map 1'. The main content is a table with columns 'DSO', 'Slot', 'Port', and 'Rbs'. The table lists 20 slots. Slot 1 is assigned to '1:FXS'. Slots 2-4 are assigned to 'open'. Slots 5-20 are assigned to 'open'. The 'Port' column shows 'unassigned' for all slots except slot 1, which is 'Router'. The 'Rbs' column shows '0n' for slot 1 and 'n/a' for all other slots. At the bottom left, it says 'MODE: Channelbank'. At the bottom right, it says 'NE1: down' and '^Z=help 0:48'.

DSO	Slot	Port	Rbs
1	1:FXS	Router	0n
2	open	unassigned	n/a
3	RCU:TA600	Router	n/a
4	open	unassigned	n/a
5	RCU:TA600	0.35	n/a
6	open	unassigned	n/a
7	open	unassigned	n/a
8	open	unassigned	n/a
9	open	unassigned	n/a
10	open	unassigned	n/a
11	open	unassigned	n/a
12	open	unassigned	n/a
13	open	unassigned	n/a
14	open	unassigned	n/a
15	open	unassigned	n/a
16	open	unassigned	n/a
17	open	unassigned	n/a
18	open	unassigned	n/a
19	open	unassigned	n/a
20	open	unassigned	n/a

MODE: Channelbank
NE1: down
^Z=help 0:48

Figure 14. Enter Map Menu

DSO

Displays the network T1 time slot to be assigned.

Slot

When you select this option, a list of all of the slots displays. The first option is **open**, which unassigns the slot if selected. The second option is **FXS**. The slot number and name are shown. For example, **1: FXS** indicates that FXS is in slot 1. The next options allow mapping of interfaces controlled by the RCU. Use **RCU:Total Access 600** to map network timeslots to the V.35 port or to the router. Pick the appropriate slot and press **Enter**.

Port

When you select this option, a list of ports and module types appears. Pick the appropriate port and module type, and press **Enter**. The selection list shows only the remaining ports available to be assigned. It may be necessary to unassign a port in order to reassign it elsewhere.

RBS

(Robbed Bit Signaling) Defines whether the connection has active RBS. Where RBS is not an option, TA 600 automatically assigns the correct setting. For example, a V.35 connection is set to **Off**.

ON Preserves the signaling bits between the connections.

OFF Ignores signaling bits.

V.35 Setup

The **V.35 SETUP** menu allows you to configure the V.35 port. Figure 15 on page 49 shows the **V.35 SETUP** menu.

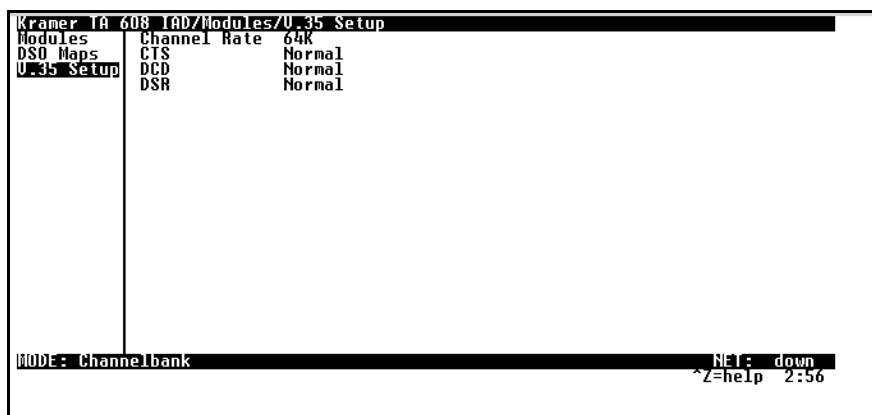


Figure 15. V.35 Setup Menu

Channel Rate

Sets the base rate of the V.35 interface. Choices are **64K** or **56K**. This determines the ultimate rate the V.35 port will be clocked at, depending on the number of timeslots mapped to the port. For example, if 64K is selected here and 4 timeslots are mapped to V.35 on the active DS0 map, the V.35 will be clocked at 256K.

CTS

Sets the control characteristic of the clear-to-send lead. Choices are **NORMAL** (follows RTS) or **FORCE ON**.

DCD

Sets the control characteristic of the carrier detect lead. Choices are **NORMAL** (follows valid signal on the network interface) or **FORCE ON**.

DSR

Sets the control characteristic of the data set ready lead. Choices are **NORMAL** (follows DTR) or **FORCE ON**.

Appendix A. Updating Total Access 600 Firmware using XMODEM

The Total Access 600 supports firmware updating using XMODEM transfer protocol via the base unit's **CRAFT** port. XMODEM is found in the VT 100 terminal emulation application in the ADTRAN Utilities package and in most PC VT 100 communications software packages.



Make certain that the communications software package used has flow control turned off.

Before beginning this procedure, you must obtain the appropriate update file from ADTRAN Technical Support at **(888) 4ADTRAN (423-8726)**.

An XMODEM download can be initiated by enabling a forced download or by using the console menus. The following materials are required.

- VT 100 terminal or PC with VT 100 terminal emulation software
- XMODEM software



To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

Updating Firmware via a Forced Download

Perform the Steps Below in the Order Listed

1. **Using a VT 100 terminal emulation communication software package which contains XMODEM protocol support, log in to TA 600. Set the transmit rate of the emulation software to 9600 baud.**
2. **Unplug the unit to remove power. When power is reapplied, hold down the letter 'B' from the VT 100 terminal. Before the unit begins its boot-up sequence it will check for the letter 'B'. If present, the download menu will appear.**



Both uppercase and lowercase letters will work for the Forced Download. Make certain flow control is disabled for the VT 100 interface.

3. Press Enter until a menu appears.



*To shorten transmit time, select the option from the menu to change the transmit rate to 115.2K baud or the highest rate supported by the terminal emulation software. If this transmit rate is changed, change emulation software properties to match this rate and disconnect and connect again. Press **Enter** again until the menu appears.*

4. Choose option 1, **BEGIN XMODEM DOWNLOAD Now**, from the menu to start the XMODEM file download.
5. Press **Y** at the **START FLASH DOWNLOAD NOW** prompt to continue with the XMODEM file transfer.



*When Total Access 600 is ready to receive the XMODEM upload, the menu screen will display **Transmit Flash . . . download file now**. If this does not appear, please review the steps above for possible configuration errors.*

6. From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to terminal emulation software documentation for help. Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully.)



*Because XMODEM data is being transferred in-band through the menu interface, the VT 100 menus of Total Access 600 will be inoperable from the **CRAFT** port.*

7. When the update has successfully completed, **TRANSFER COMPLETE** appears in the terminal window. If an error occurs during the update, an error message will display in the terminal window. If this occurs, return to Step 3 and attempt the update again. If the same error occurs, contact ADTRAN Technical Support.
8. After the **TRANSFER COMPLETE** message has been displayed, cycle power on the unit.

9. **Change the emulation software properties to 9600 baud. Disconnect and connect to the unit at this transmit rate and continue configuring the unit as normal.**



It is suggested that a factory default be conducted after the unit is updated with new firmware.

Updating Firmware via the Console Menus

1. **Using a VT 100 terminal emulation communication software package which contains XMODEM protocol support, log in to TA 600.**
2. **Select SYSTEM UTILITY/UPDATE FIRMWARE.**
3. **Select XMODEM for TRANSFER METHOD.**
4. **Press Enter on START TRANSFER <+>.**
5. **When prompted, press Y to erase flash.**



*When Total Access 600 is ready to receive the XMODEM upload, the menu screen will clear and display **Transmit Flash . . . download file now**. If this does not appear, please review the steps above for possible configuration errors.*

6. **From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to terminal emulation software documentation for help. Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully.)**



*Because XMODEM data is being transferred in-band through the menu interface, the VT 100 menus of Total Access 600 will be inoperable from the **CRAFT** port.*

7. **When the update has successfully completed, TRANSFER COMPLETE displays in TRANSFER STATUS. The module restarts immediately and resumes operation. If an error occurs during the update, an error message will display in the TRANSFER STATUS field. If this occurs, return to Step 3 and attempt the update again. If the same error occurs, contact ADTRAN Technical Support.**

Appendix B. Updating Total Access 600 Firmware using TFTP

TA 600 supports firmware updates via the IP network using TFTP from a network server. The network server must be capable of supporting TFTP server requests from the TFTP client within the TA 600.

You must have a level 2 password to perform updates to the Total Access 600. Please consult the Total Access 600 administrator if this password is not known.

You must obtain the appropriate update file from ADTRAN Technical Support at **(888) 4ADTRAN (423-8726)**.

You must copy the update file provided by ADTRAN to a network server that supports TFTP server requests. Record both the IP address of the server and the full path location of the update file to be downloaded.

The following materials are required.

- A PC with a Telnet client software
- A TFTP Server accessible on the local network (a TFTP Server is provided as part of the ADTRAN Utilities software)

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.



CAUTION

Electronic modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electronic components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them on an approved antistatic mat that is electrically grounded.

Perform Steps Below in the Order Listed

1. **Using a Telnet program, log in to Total Access 600.**
2. **Select SYSTEM UTILITY / UPDATE FIRMWARE.**
3. **Select TFTP for TRANSFER METHOD.**
4. **Enter into TFTP SERVER IP ADDRESS, the IP address of the network server that was recorded earlier.**
5. **Enter into TFTP SERVER FILENAME, the full path name and filename of the update file that was recorded earlier.**
6. **Select START TRANSFER <+> to start the update process. Enter Y to confirm the transfer and to set up the module to receive the TFTP upload.**



*During the TFTP upload process, various status messages display in **CURRENT UPDATE STATUS** to indicate progress. The table below describes these messages.*

When the update has successfully completed, **TRANSFER COMPLETE** displays in **TRANSFER STATUS**. The Total Access 600 restarts immediately and resumes operation.

If an error occurs during the update, an error message will display in the **TRANSFER STATUS** field. If this occurs, return to Step 3 and attempt the update again. If the same error occurs, contact ADTRAN Technical Support.

During the TFTP upload, various status messages display to indicate progress. The following table describes these messages.

Message	Meaning
Contacting Server	Indicates communication with the TFTP network server is trying to be established with the specified server address in the TFTP Server IP Address field.
Beginning TFTP Transfer	Indicates communication with the TFTP network server has been established and the update file is being transferred between Total Access 600 and the TFTP network server.
Completed	Indicates the Total Access 600 product successfully received the update file.

Message	Meaning
Error: File Not Found	Indicates the TFTP network server was unable to locate the specified file name or path in the TFTP Server File-name field.
Error: Access Violation	Indicates the TFTP network server denied Total Access 600 access to the given update file name and path. Please verify appropriate user rights are selected for the specified path.
Error: Illegal Operation	An unknown operation was detected by Total Access 600 when transferring the update file from the TFTP network server.
Error: User Aborted	Indicates the user selected CANCEL UPDATE to abort reception of the update file from the TFTP network server.

Appendix C. Navigating the Terminal Menus

Terminal Menu Window

The TA 600 uses a multilevel menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window, through which you have complete control of the TA 600 (see Figure 16).

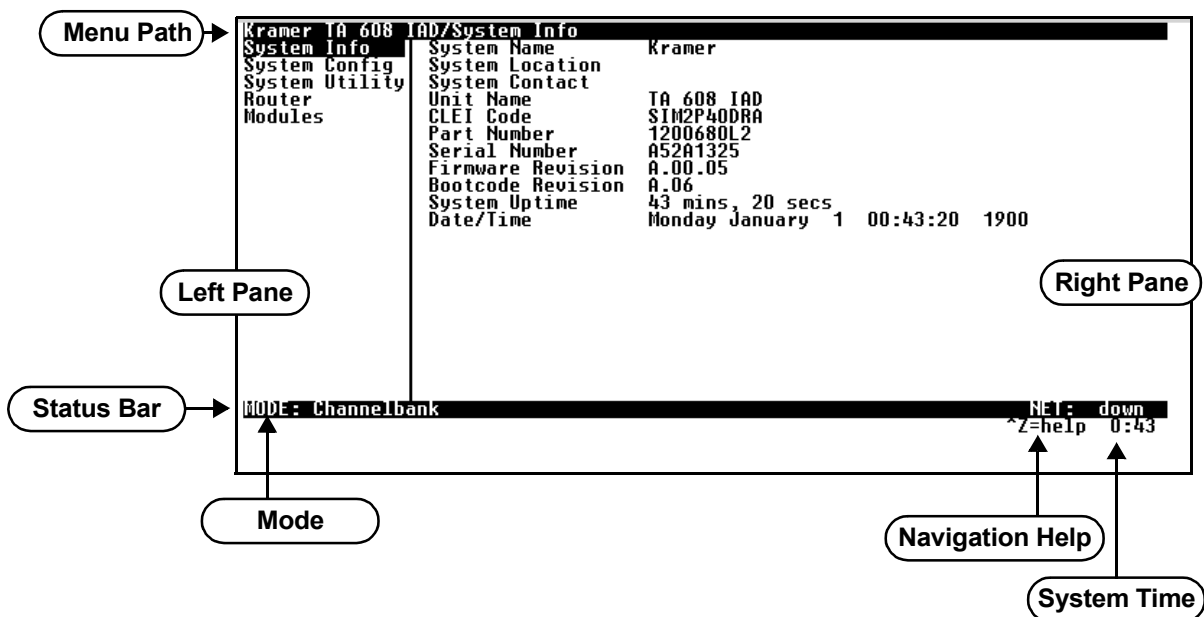


Figure 16. Top-level Terminal Menu Window

Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 16 shows the top-level menu with the cursor on the **SYSTEM INFO** submenu; therefore, the menu path reads **TOTAL ACCESS 600/SYSTEM INFO**.



The top level menu path will always display the specific product name from the Total Access 600 family.

Window Panes

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

Window Pane Navigation

Use the following chart to assist you in moving between and within the two window panes.

To move...	Press one of these keys...
From left pane to right pane	Tab Enter Right arrow
From right pane to left pane	Tab Escape Left arrow
Within each pane	Up arrow Down arrow Left arrow Right arrow

Right Window Pane Notation

The right window pane shows the contents of the currently selected menu. These contents can include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

This notation...	Means that...
[+]	More items are available when selected.
[DATA]	More items are available when selected.
<+>	An action is to be taken, such as activating a test.
Highlighted menu item	You can enter data in this field.
Underlined field	The field contains read-only information.

Additional Terminal Menu Window Features

Mode	Describes the mode of the Total Access 600 base unit (system).
Port Status	Indicates the types of modules installed in ports 1—6.
Navigation Help	Lists characters used for navigating the terminal menu (Ctrl-Z). See also <i>Moving through the Menus</i> on page 58.
System Time	Displays current time. See <i>Date/Time</i> on page 19 for details on editing the time.

Navigating Using the Keyboard Keys

You can use various keystrokes to move through the terminal menus, to manage a terminal menu session, and to configure the system. Press **Ctrl-Z** to activate a pop-up screen listing the navigation keystrokes.

Moving through the Menus

To do this...	Press this key...
Return to the home screen.	H
Jump between two menu items. Press J while the cursor is located on a menu item, and you jump back to the main screen. Go to another menu item, press J , and you jump back to the screen that was displayed the first time you pressed J . Press J when you want to jump between these items.	J
Select items.	Arrows
Edit a selected menu item.	Enter
Cancel an edit.	Escape
Close pop-up help screens.	Escape
Move between the left and right panes.	Tab or Arrows
Move to the top of a screen.	A
Move to the bottom of a screen.	Z
Ascend one menu level.	Backspace

Session Management Keystrokes

To do this...	Press this...
Log out of a session.	Ctrl-L
Invalidate the password entry and return to the login screen.	Ctrl-S
Refresh the screen. To save time, only the portion of the screen that has changed is refreshed. This option should be necessary only if the display picks up incorrect characters.	Ctrl-R

Configuration Keystrokes

To do this...	Press this key...
<p>Restore factory default settings.</p> <p>This setting restores the factory defaults based on the location of the cursor. If the cursor is on a module line (in the MODULES menu), then only the selected module is updated to factory defaults.</p>	F
<p>Copy selected items to the clipboard.</p> <p>The amount of information you can copy depends on the cursor location when you press C:</p> <ul style="list-style-type: none"> • If the cursor is over an editable field, only that item is copied. • If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the SLOT # field in the MODULES screen, all of the information associated with the slot is copied. 	C
<p>Paste the item stored in the clipboard, if the information is compatible.</p> <p>You must confirm all pastes—except those to a single editable field.</p>	P
Increment the value of certain types of fields by one when you paste information into those fields.	>
Decrement the value of certain types of fields by one when you paste information into those fields.	<
<p>Insert a new list item.</p> <p>For example, add a new item to the DLCI MAPPING by pressing I while the cursor is over an index number.</p>	I
<p>Delete a list item.</p> <p>For example, delete an item from the DLCI MAPPING by pressing D while the cursor is over the index number.</p>	D

Getting Help

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, **^A** displays at the bottom of the window. At this point, if you press **Ctrl-A**, a pop-up help screen displays with information about the item.



Press **Ctrl-Z** to activate the help screen that displays the available keystrokes you can use to navigate the terminal menus.

Appendix D. Configuring the Total Access 600 for Routing

Initial Setup

Before the Total Access 600 can be configured for routing, DS0s must be mapped to the system controller or RCU. (See *DS0 Mapping* below.)

DS0 Mapping

DS0 Mapping Instructions	
Step	Action
1	From the Main menu, select CHANNEL BANK and then select DS0 MAPS .
2	Set the VIEW/EDIT MAP to either MAP 1 or MAP 2 , based on which map you want to edit. The unit can store two maps.
3	Set the USE AS TEMPLATE option as described below. <ul style="list-style-type: none">To start a new map, use a CLEAR MAP as a template.To edit or update an existing map, use either CURRENT MAP 1 or CURRENT MAP 2 as a template. (Press Enter while CLEAR MAP is highlighted to view these options.)
4	Press Enter on the ENTER MAP [+] option to view the map.
 NOTE	<i>The T1 line entering the Total Access 600 is broken up into 24 DS0s or channels. At least one DS0 needs to be mapped to the router in order to use the unit for routing purposes.</i>
5	Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.)
6	Set the SLOT number of the DS0 that you are mapping to RCU: TOTAL ACCESS 600 .
7	Set the PORT of the DS0 that you are mapping to ROUTER .
8	Map all the DS0s as desired, and exit this menu by pressing the left arrow button.
 NOTE	<i>When it asks to update the map, choose Y if you would like to save your changes, or N if you want to restore the previous map.</i>
9	Make sure the ACTIVE MAP is set to the correct map (the map you want running) before exiting the CHANNEL BANK/DS0 MAPS menu.

Setting up Routing Options

Choose one of the following options, based on how the Total Access 600 will be used for routing: (a) IP Routing, (b) IPX Routing, (c) IP and IPX Routing, and (d) No Routing. All of these procedures are described on the pages that follow.

IP Routing

There are three steps required for the Total Access 600 to be used for IP Routing: (1) Global IP Setup, (2) Ethernet IP Setup, and (3) WAN IP Setup. All of these procedures are described in the pages that follow.

Global IP Setup

Global IP Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select GLOBAL .
2	Press Enter on the IP [+] option.
3	Set the MODE to ON .
4	Press Enter on the STATIC ROUTES [+] to place static routes in the routing table.


Ethernet IP Setup

Ethernet IP Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select ETHERNET .
2	Press Enter on the IP [+] option.
3	Set the IP ADDRESS of the Ethernet port.
4	Set the SUBNET MASK of the Ethernet port.
5	Set the DEFAULT GATEWAY of the Ethernet port if needed.
6	Press Enter on the RIP [+] option.
7	Set the MODE to ON or OFF based on whether you want RIP enabled. If you choose to enable RIP, then continue to set the following options.
8	Set the PROTOCOL to V1 or V2 .
9	Set the METHOD to NONE , SPLIT HORIZON , or POISON REVERSE .
10	Set the DIRECTION to TX ONLY , Rx ONLY , or TX AND Rx .
11	Set the V2 SECRET or password.
12	Press the left arrow key to return to the ETHERNET/IP menu, and then set the PROXY ARP to YES or NO .

WAN IP Setup

For WAN IP setup, choose either PPP IP Setup or Frame Relay IP Setup. Both of these procedures are described on the pages that follow.

WAN IP Setup - PPP IP Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to PPP .
3	Press Enter on the PPP PROFILE [+] option.
4	Press Enter on the AUTHENTICATION [+] option if you wish to change options related to how the link is established.
5	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the IP [+] option.
6	Set the MODE to ON .
7	Press Enter on the RIP IP [+] option.
8	Set the MODE to ON or OFF based on whether you want RIP enabled. If you choose to enable RIP, then continue to set the following options.
9	Set the PROTOCOL to V1 or V2 .
10	Set the METHOD to NONE , SPLIT HORIZON , or POISON REVERSE .
11	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the FILTERS [+] option to set filters if you choose to do so.

WAN IP Setup - Frame Relay IP Setup Instructions	
(required if the Total Access 600 is to be used for Frame Relay IP Routing on the WAN interface)	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to FRAME RELAY .
3	Press Enter on the FRAME RELAY [+] option .
4	Set the MAINTENANCE PROTOCOL to ANNEX D, ANNEX A, LMI, OR STATIC .
 NOTE	<i>The MAINTENANCE PROTOCOL should be set based on the Frame Relay switch.</i>
5	Set the Maintenance DLCI if you want to change it from the default setting.
6	Now you must choose either to Map DLCIs or Learn DLCIs. These procedures are described below.

Frame Relay IP Setup - Map DLCIs	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and press Enter on the FRAME RELAY [+] option .
2	Press Enter on DLCI MAPPING [+] .
3	Set ACTIVE to YES .
4	Set DLCI to the DLCI number.
5	Press Enter on the IP MAP [+] .
6	Set ACTIVE to YES .
7	Set IARP to YES or NO .
8	Set the FAR-END IP ADDRESS .
9	Set the IP NETMASK .
10	Set the LOCAL IP ADDRESS .
11	Set the RIP PROTOCOL if you want to enable RIP on this DLCI.
12	If you choose to enable RIP, set the RIP METHOD and the RIP DIRECTION .
13	Set NAT to either ON or OFF .
14	Repeat these steps until the DLCI Map is complete.

Frame Relay IP Setup - Learn DLCIs

When Inverse ARP is enabled (by default), the Total Access 600 can learn the DLCI number of a route. Allowing the unit to learn the DLCI number revokes all configuration capabilities of that DLCI.
--

IPX Routing

There are three steps required for the Total Access 600 to be used for IPX Routing: (1) Global IPX Setup, (2) Ethernet IPX Setup, and (3) WAN IPX Setup. All of these procedures are described on the pages that follow.

Global IPX Setup

Global IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select GLOBAL .
2	Set the IPX MODE to ON .


Ethernet IPX Setup

Ethernet IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select ETHERNET .
2	Press Enter on the IPX [+] option.
3	Set the NETWORK of the Ethernet port.
4	Set the FRAME TYPE of the Ethernet port.
5	Set the SEED STATUS of the Ethernet port if needed.
6	Set the RIP TIMER .
7	Set the SAP TIMER .

WAN IPX Setup

For the WAN IPX setup, choose either PPP IPX Setup or Frame Relay IPX Setup. Both of these procedures are described on the pages that follow.

WAN IPX Setup - PPP IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to PPP .
3	Press Enter on the PPP PROFILE [+] option.
4	Press Enter on the AUTHENTICATION [+] option if you wish to change options related to how the link is established.
5	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the IPX [+] option.
6	Set the MODE to ON .
7	Set the REMOTE NETWORK .
8	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the FILTERS [+] option to set filters if you choose to do so.

WAN IPX Setup - Frame Relay IPX Setup Instructions	
(required if the Total Access 600 is to be used for Frame Relay IPX Routing on the WAN interface)	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to FRAME RELAY .
3	Press Enter on the FRAME RELAY [+] option .
4	Set the MAINTENANCE PROTOCOL to ANNEX D, ANNEX A, LMI, OR STATIC .
 NOTE	<i>The MAINTENANCE PROTOCOL should be set based on the Frame Relay switch.</i>
5	Set the Maintenance DLCI if you want to change it from the default setting.
6	Now you must choose either to Map DLCIs or Learn DLCIs. These procedures are described below.

Frame Relay IPX Setup - Map DLCIs	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and press Enter on the FRAME RELAY [+] option .
2	Press Enter on DLCI MAPPING [+] .
3	Set ACTIVE to YES .
4	Set DLCI to the DLCI number.
5	Press Enter on the IPX MAP [+] .
6	Set ACTIVE to YES .
7	Set IARP to Yes or No .
8	Set the LINK NETWORK .
9	Repeat these steps until the DLCI Map is complete.

Frame Relay IPX Setup - Learn DLCIs

When Inverse ARP is enabled (by default), the Total Access 600 can learn the DLCI number of a route. Allowing the unit to learn the DLCI number revokes all configuration capabilities of that DLCI.
--

IP and IPX Routing

There are three steps required for the Total Access 600 to be used for IP and IPX Routing: (1) Global IP and IPX Setup, (2) Ethernet IP and IPX Setup, and (3) WAN IP and IPX Setup. All of these procedures are described on the pages that follow.

Global IP and IPX Setup

Global IP and IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select GLOBAL .
2	Press Enter on the IP [+] option.
3	Set the MODE to ON .
4	Press Enter on the STATIC ROUTES [+] to place static routes in the routing table.
5	Set the IPX MODE to ON .


Ethernet IP and IPX Setup

Ethernet IP and IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select ETHERNET .
2	Press Enter on the IP [+] option.
3	Set the IP ADDRESS of the Ethernet port.
4	Set the SUBNET MASK of the Ethernet port.
5	Set the DEFAULT GATEWAY of the Ethernet port if needed.
6	Press Enter on the RIP [+] option.
7	Set the MODE to ON or OFF based on whether you want RIP enabled. If you choose to enable RIP, then continue to set the following options.
8	Set the PROTOCOL to V1 or V2 .
9	Set the METHOD to NONE , SPLIT HORIZON , or POISON REVERSE .
10	Set the DIRECTION to TX ONLY , Rx ONLY , or Tx AND Rx .
11	If using a V2 password, set the V2 SECRET .
12	Press the left arrow key to return to the ETHERNET/IP menu, and then set the PROXY ARP to YES or No .
13	Press the left arrow key to return to the ETHERNET/IP menu, and then press Enter on the IPX [+] option.
14	Set the NETWORK of the Ethernet port.
15	Set the FRAME TYPE of the Ethernet port.
16	Set the SEED STATUS of the Ethernet port if needed.
17	Set the RIP TIMER .
18	Set the SAP TIMER .

WAN IP and IPX Setup

For WAN IP and IPX Setup, choose either PPP IP and IPX Setup or Frame Relay IP and IPX Setup. Both of these procedures are described on the pages that follow.

WAN IP and IPX Setup - PPP IP and IPX Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to PPP .
3	Press Enter on the PPP PROFILE [+] option.
4	Press Enter on the AUTHENTICATION [+] option if you wish to change options related to how the link is established.
5	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the IP [+] option.
6	Set the MODE to ON .
7	Press Enter on the RIP IP [+] option.
8	Set the MODE to ON or OFF based on whether you want RIP enabled. If you choose to enable RIP, then continue to set the following options.
9	Set the PROTOCOL to V1 or V2 .
10	Set the METHOD to NONE , SPLIT HORIZON , or POISON REVERSE .
11	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the IPX [+] option.
12	Set the MODE to ON .
13	Set the REMOTE NETWORK .
14	Press the left arrow key to return to the WAN/PPP PROFILE menu, and then press Enter on the FILTERS [+] option to set filters if you choose to do so.

WAN IP and IPX Setup - Frame Relay IP and IPX Setup Instructions (required if the Total Access 600 is to be used for Frame Relay IP and IPX Routing on the WAN interface)	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to FRAME RELAY .
3	Press Enter on the FRAME RELAY [+] option.
4	Set the MAINTENANCE PROTOCOL to ANNEX D, ANNEX A, LMI, OR STATIC .
 NOTE	<i>The MAINTENANCE PROTOCOL should be set based on the Frame Relay switch.</i>
5	Set the Maintenance DLCI if you want to change it from the default setting.
6	Now you must choose either to Map DLCIs or Learn DLCIs. These procedures are described on the next page.

Frame Relay IP and IPX Setup - Map DLCIs	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and press Enter on the FRAME RELAY [+] option.
2	Press Enter on DLCI MAPPING [+] .
3	Set ACTIVE to YES .
4	Set DLCI to the DLCI number.
5	Press Enter on the IP MAP [+] .
6	Set ACTIVE to YES .
7	Set IARP to YES or NO .
8	Set the FAR-END IP ADDRESS .
9	Set the IP NETMASK .
10	Set the LOCAL IP ADDRESS .
11	Set the RIP PROTOCOL if you want to enable RIP on this DLCI.
12	If you chose to enable RIP, set the RIP METHOD and the RIP DIRECTION .
13	Set NAT to either ON or OFF .
14	Press Enter on the IPX MAP [+] .
15	Set ACTIVE to YES .
16	Set IARP to YES or NO .
17	Set the LINK NETWORK .
18	Repeat these steps until the DLCI Map is complete.

Frame Relay IP and IPX Setup - Learn DLCIs
When Inverse ARP is enabled (by default), the Total Access 600 can learn the DLCI number of a route. Allowing the unit to learn the DLCI number revokes all configuration capabilities of that DLCI.

Appendix E. Configuring the Total Access 600 for Bridging

Initial Setup

Before the Total Access 600 can be configured for bridging, DS0s must be mapped to the system controller or RCU. (See *DS0 Mapping* on page 60).

Setting up Bridging Options

If the Total Access 600 will be used for bridging, continue with the steps below.

Bridging

There are two steps required for the Total Access 600 to be used for Bridging: (1) Global Bridging Setup and (2) WAN Bridging Setup. Both of these procedures are described on the pages that follow.


Global Bridging Setup

Global Bridging Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select GLOBAL .
2	Press Enter on the BRIDGE [+] option.
3	Set the MODE to ON .

WAN Bridging Setup

Choose one of the following options: PPP Bridge Setup or Frame Relay Bridge Setup. Both of these procedures are described on the pages that follow.

WAN Bridging - PPP Bridge Setup Instructions	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to PPP .
3	Press Enter on the PPP PROFILE [+] option.
4	Press Enter on the BRIDGE [+] option.
5	Set the MODE to ON .

WAN Bridging - Frame Relay Bridge Setup Instructions	
(required if the Total Access 600 is to be used for Frame Relay IP Routing on the WAN interface)	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , and then select WAN .
2	Set the L2 PROTOCOL to FRAME RELAY .
3	Press Enter on the FRAME RELAY [+] option.
4	Set the MAINTENANCE PROTOCOL to ANNEX D, ANNEX A, LMI, OR STATIC .
 NOTE	<i>The MAINTENANCE PROTOCOL should be set based on the Frame Relay switch.</i>
5	Set the Maintenance DLCI if you want to change it from the default setting.
6	Now you must choose either to Map DLCIs or Learn DLCIs. These procedures are described below.

Frame Relay Bridge Setup - Map DLCIs	
Step	Action
1	From the Main Menu, select ROUTER , select CONFIG , select WAN , and press Enter on the FRAME RELAY [+] option.
2	Press Enter on DLCI MAPPING [+] .
3	Press Enter on the BRIDGE MAP [+] of each DLCI you wish to set up for bridging.
4	Set ACTIVE to YES .
5	Set the BRIDGE GROUP .

Frame Relay Bridge Setup - Learn DLCIs
When Inverse ARP is enabled (by default), the Total Access 600 can learn the DLCI number of a route. Allowing the unit to learn the DLCI number revokes all configuration capabilities of that DLCI.


No Bridging

You have chosen not to use the Total Access 600 for bridging.



Appendix F. Configuring the Total Access 600 for Operation with Voice Modules

To set the Total Access 600 up for operation with voice modules, follow the steps below.

Mapping the DS0s



DS0 Mapping Instructions	
Step	Action
1	From the MODULES menu, select DS0 MAPS .
2	Set DS0 MAPS to ENTER MAP 1 or ENTER MAP 2 , based on which map you want to edit. The unit can store two maps.
3	<ul style="list-style-type: none"> To start a new map, use a CLEAR MAP as a template. To edit or update an existing map, use either ENTER MAP 1 or ENTER MAP 2 as a template.
4	Press Enter on the ENTER MAP [+] option to view the map.
 NOTE	<i>The T1 line entering the Total Access 600 is broken up into 24 DS0s or channels. You must map each voice port you want to use.</i>
5	Scroll down to the DS0 that will be mapped.
6	Set the PORT of the DS0 that you are mapping. The port number entered must match the voice port the DS0 is being mapped to. RBS (robbed bit signalling) will automatically turn on when a port number has been selected.
7	Map all the DS0s as desired, and exit this menu by pressing the left arrow key.
8	Make sure the ACTIVE MAP is set to the map definition you want implemented before exiting the DS0 MAPS menu.

Setting up the NET (T1) Module

NET (T1) Module Setup Instructions	
Step	Action
1	From the Main Menu, select MODULES .
2	Enter the MENU column of NET (T1) Module. (Details of the NET port will be displayed.)
3	Set the FORMAT of the NET port to ESF , SF , or SLC96 .
 NOTE	<i>This format must match the format used by the other units in the network.</i>
4	Set the LINE CODE of the NET port to B8ZS or AMI .
 NOTE	<i>This line code must match the line code used by the other units in the network.</i>
5	Set the EQUALIZATION or line build out in the lines based on the size of the network.
6	Set the CSU LOOPBACK option to ENABLE or DISABLE based on whether looping to this unit from another unit will be allowed.

Now go to *Setting up the FXS Voice Ports* on page 77.

Setting up the FXS Voice Ports

FXS Voice Ports Setup Instructions	
Step	Action
1	From the Main Menu, select MODULES .
2	Enter the MENU column of the FXS MODULE . (Details of the four/eight voice ports will be displayed.)
3	Set the MODE of each port to LOOP START , GROUND START , or TANDEM (E&M) .
 NOTE	<p><i>This mode needs to be set based on how the network is set up and how each port is being used. Each port does not need to be set to the same mode.</i></p> <p><i>If the mode is set to TANDEM (E&M), be sure to set the TANDEM options as described in Steps 8 and following.</i></p>
4	Set the Tx (dB) or transmit direction level points of each port.
5	Set the Rx (dB) or receive direction level points of each port.
6	Set the Svc MODE of each port to either IN SERVICE or OUT OF Svc .
7	Set the LINE Z , or line impedance, of each port based on the size of the network.
8	Press Enter on the TANDEM [+] option to view the TANDEM options if the port mode is set to TANDEM (E&M) .
9	Set the CONVERSION MODE of the port to either LOOP START or GROUND START .
10	Set the SUPERVISION of the port to either IMMEDIATE or WINK .
 NOTE	<p><i>Be sure to set the TANDEM options for each port set to TANDEM E&M.</i></p>

Appendix G. Craft Port Connection Pin-Out

DB-9	RJ-45	Description
2	5	TX Data
3	3	RX Data
5	1	GND
Note: All other pins are unused.		